Approved: _____ ORIGINAL
JENNIFER L. BEIDEL
Assistant United States Attorney

Before: THE HONORABLE ROBERT W. LEHRBURGER
United States Magistrate Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

18 MAG 9599

UNITED STATES OF AMERICA	**SEALED COMPLAINT**
- v. -	Violation of 18 U.S.C. § 1349
YENDOUKOA LAMBONI,	
Defendant.	COUNTY OF OFFENSE: NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

KRISTIN ALLAIN, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation (the "FBI"), and charges as follows:

COUNT ONE
(Conspiracy to Commit Wire Fraud and Bank Fraud)

1. From in or about November 2016 through in or about November 2018, in the Southern District of New York and elsewhere, YENDOUKOA LAMBONI, the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud and bank fraud, in violation of Title 18, United States Code, Sections 1343 and 1344, to wit, LAMBONI opened bank accounts in the names of sham companies to receive fraud proceeds and distributed those proceeds to himself.

2. It was a part and an object of the conspiracy that YENDOUKOA LAMBONI, the defendant, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses,

representations, and promises, would and did transmit and cause to be transmitted by means of wire and radio communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

3. It was further a part and an object of the conspiracy that YENDOUKOA LAMBONI, the defendant, and others known and unknown, willfully and knowingly, would and did execute a scheme and artifice to defraud a financial institution and to obtain moneys, funds, credits, assets, securities and other property owned by, and under the custody and control of, a financial institution, by means of false and fraudulent pretenses, representations and promises, in violation of Title 18, United States Code, Section 1344.

(Title 18, United States Code, Section 1349.)

4. I am a Special Agent with the FBI. This Complaint is based upon my personal participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals. Because this Complaint is being submitted for the limited purpose of demonstrating probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

The Business Email Compromise Scheme

5. Based on my experience and involvement in the investigation, a Business Email Compromise ("BEC") scheme is a scheme by which a target spoofs a company email account to defraud the company or its employees, customers, or vendors of money.

6. Based on my involvement in this investigation, and as discussed in further detail below, the perpetrators of the BEC scheme used an email account ("the BEC Email Account") in furtherance of the scheme. The perpetrators sent emails from the BEC Email Account that appeared as if they came from other legitimate companies' email accounts. To accomplish this, the users of the BEC Email Account altered the sender information on the emails they sent from the BEC Email Account, a process known as email "spoofing." If, for example, the users of the BEC Email Account wanted their emails to appear as if they came from

"johndoe@company.com," they would alter the sender information to reflect that the email was sent from "johndoe@company.com," even though the email was not actually sent from that account, and then carbon copy a similar email address such as "johndoe.company@usa.com." All replies to the carbon copied email address, in this case for the purposes of example, "johndoe.company@usa.com," were set to automatically forward to the BEC Email Account, so that the users of the BEC Email Account could maintain a dialogue with their victims. Using this process, the users of the BEC Email Account corresponded with victims regarding the payment of actual debts that the victims owed to legitimate companies using emails that appeared to come from those legitimate companies. This correspondence often tricked those victims into paying those debts via wire transfers to accounts controlled by the users of the BEC Email Account.

7. Based on my interviews with victims of the BEC scheme and review of email correspondence provided by those victims and bank records obtained via grand jury subpoena, I am aware of the following:

a. Prior to in or about December 2017, a vendor ("Victim-1") provided conference-planning services to a non-profit institution ("Victim-2"). Victim-2 is headquartered in New York, New York.

b. Beginning in at least June 2017, the Executive Director of Victim-1 and the then-Treasurer of Victim-2[1] corresponded regarding payment for expenses related to a conference using the email address "mike.[redaction 1]@[redaction 1].com,"[2] among other email addresses. Ultimately, Victim-1 would bill Victim-2 approximately $390,000 for the conference-planning services.

c. On or about September 25, 2017, Victim-1, using the email address "mike.[redaction 1]@[redaction 1].com," provided wiring instructions directing that Victim-2 send

---

[1] All actions taken by Victim-1 and Victim-2 throughout this Complaint were conducted by the Executive Director of Victim-1 and the then-Treasurer of Victim-2.

[2] The Government has removed words that would identify victims from the email addresses at issue. Where the phrase "[redaction 1]" appears, Victim-1's surname was removed. Where the phrase "[redaction 2]" appears, Victim-4's surname was removed.

payment to a bank account at a particular financial institution ("Bank-1"). A representative of Victim-1 has confirmed that the bank account referenced at Bank-1 in fact belongs to Victim-1.

d. On or about December 14, 2017 and on or about January 3, 2018, the email account "mike.[redaction 1].[redaction 1]@usa.com" emailed Victim-2, requesting that payment of the over $120,000 balance owed to Victim-1 be redirected to a bank account at a different financial institution ("Bank-2"). Victim-2 made the payment ("the Payment") to the Bank-2 account provided in the emails sent from the "mike.[redaction 1].[redaction 1]@usa.com" email account.

e. On or about January 24, 2018, Victim-1 contacted Victim-2 to inquire regarding when Victim-2 would be paying the approximately $120,000 balance. Victim-2 stated that Victim-2 had already paid the approximately $120,000 balance to Bank-2 via the Payment. Victim-1 explained that Victim-1 had not received the Payment and had not written the emails referenced in paragraph 7(d) above.

f. Upon further inquiry, Victim-2 discovered that the emails requesting the Payment had come from "mike.[redaction 1].[redaction 1]@usa.com" when Victim-1's true email address was "mike.[redaction 1]@[redaction 1].com."

8. Based on interviews conducted by others of a victim of the BEC scheme and on my review of email correspondence provided by that victim, I am aware of the following:

a. In or about November 2017, an individual ("Victim-3") was planning to invest in several companies and began to engage in email correspondence with the managers of those companies, one of which was located in White Plains, New York ("Victim-4"). Victim-3 resided in New York, New York at all times relevant to this complaint.

b. In or about December 2017, Victim-3 received an email that was purportedly from Victim-4. The email requested that Victim-3 send her investment to a specific bank account in the name of an entity that resembled, but was not exactly the name of, Victim-4. The email also appeared to originate from "d[redaction 2]@downtownlp.com" but replies were directed to "d[redaction 2].downtownlp@usa.com." Based on the unusual characteristics of the email, Victim-3 discovered the fraud and did not make the requested payment.

9. Based on my review of written complaints made to law enforcement by an employee of a victim of the BEC scheme, I am aware of the following:

a. In or about December 2017, a bank ("Victim-5") received an email that purported to be from an escrow company ("Victim-6") that attached wire instructions for loan disbursement.

b. Victim-5 acted on the wire instructions by sending approximately $122,189. Victim-6 then called Victim-5 to inquire about the funds and learned that Victim-5 had acted on false wire instructions. Victim-5 was able to reverse the wire transaction.

10. Based on my conversations with a representative from the Internet service provider for the BEC Email Account ("the Provider"), I am aware that the Provider maintains the email account "mike.[redaction 1].[redaction 1]@usa.com." The Provider's records indicate that incoming emails to the email account "mike.[redaction 1].[redaction 1]@usa.com" automatically forwards to the BEC Email Account.

11. Based on my review of header and footer information from the BEC Email Account obtained via an Order to disclose non-content information pursuant to 18 U.S.C. § 2703(d), I am aware of the following:

a. From my review of the header and footer information provided for the period from in or about November 2016 through in or about May 2018, the vast majority of the content in the BEC Email Account appears to involved "spoofed" email addresses.

b. I found at least 90 spoofed email addresses within the BEC Email Account. Many of those spoofed email addresses are similar to email addresses used by legitimate companies in the United States and South Africa, based on research I conducted using publicly available information.

c. Among the 90 spoofed email addresses within the BEC Email Account are: (1) "mike.[redaction 1].[redaction 1]@usa.com," which was used to defraud Victim-1 and Victim-2 as discussed above; (2) "d[redaction 2].downtownlp@usa.com," which was used in an attempt to defraud Victim-3 and Victim-4, as discussed above; (3) the email address that sent the fake wire instructions to Victim-5; and (3) at least eight other email

addresses that are associated with complaints that have been made to the FBI by victims of BEC schemes.

d. Almost no legitimate content appears in the BEC Email Account. There are a few emails from the Provider, but almost no other advertising emails or non-spoofed content appears to exist in the BEC Email Account.

The Sham Bank Accounts

12. Based on my review of bank records received via grand jury subpoena from Bank-2, I am aware of the following:

a. The account holder of the Bank-2 Account is a business named SEARA-JBS Export LLC ("SEARA"), which is operated by YENDOUKOA LAMBONI, the defendant. LAMBONI is the only authorized signatory on the Bank-2 Account.

b. Bank-2 records list a seventh-floor apartment at a particular address in Silver Spring, Maryland ("the Apartment") as LAMBONI's "Residence Address," the "Statement Mailing Address" for the Bank-2 Account, and the "Street Address" for SEARA.

c. When opening the Bank-2 Account, LAMBONI described SEARA as a "home used supplys [sic]" business in the "retail trade" industry.

d. As of on or about January 8, 2018, the balance of the Bank-2 Account was approximately $10.

e. Between on or about January 10, 2018 and on or about January 16, 2018, following the approximately $120,000 payment by Victim-2 into the Bank-2 Account, LAMBONI: (1) transferred $8,000 from the Bank-2 Account to a personal account that he held at Bank-2; (2) made two over-the-counter cash withdrawals from the Bank-2 Account of $9,300 and $9,000 on or about January 10 and January 11, 2018, respectively; (3) purchased two $40,000 cashier's checks, one of which was made out to SEARA ("the SEARA Cashier's Check"), using funds from the Bank-2 Account; (4) made a payment from the Bank-2 Account to the property management company for the Apartment ("the Property Management Company") in the amount of $1,428; and (5) withdrew additional funds from the Bank-2 Account using a debit card.

13. Based on my review of bank records and security surveillance footage received via grand jury subpoena from a

bank ("Bank-3") and of official records from the Maryland Motor Vehicle Administration, I am aware of the following:

a. Bank-3 maintains an account for SEARA ("the Bank-3 Account"). YENDOUKOA LAMBONI, the defendant, is the only authorized signatory for the Bank-3 Account and is listed as the "Business Contact" for SEARA.

b. When opening the Bank-3 Account, LAMBONI described SEARA as a "homebased," "household appliance stores" business. Nonetheless, Bank-3 records list the Apartment as the "Legal Address" and the "Business Physical Address (Operating Location)" for SEARA.

c. As of on or about January 1, 2018, the balance of the Bank-3 Account was approximately $23.78.

d. On or about January 12, 2018, the SEARA Cashier's Check was deposited into the Bank-3 Account.

e. Between on or about January 16, 2018 and on or about January 31, 2018, LAMBONI: (1) made four over-the-counter cash withdrawals from the Bank-3 Account of $9,300, $9,000, $1,500, and $1,000 on or about January 16, January 17, January 20, and January 27, respectively; (2) made a payment from the Bank-3 Account to the Property Management Company in the amount of $4,550; (3) withdrew additional funds from the Bank-3 Account using a debit card; and (4) made three payments from the Bank-3 Account to PayPal in the total amount of approximately $3,400.

f. Surveillance footage from Bank-3 shows LAMBONI, whom I have identified via comparison to an official photograph of LAMBONI from his Maryland driver's license, conducting certain of the transactions referenced in the previous subparagraph.

g. The Bank-3 Account is accessible electronically through online banking services offered by Bank-3. The Bank-3 Account was accessed on at least four occasions via a particular Internet Protocol ("IP") Address ("IP Address-1"), which is a numerical label assigned to a device that can access the Internet and that uniquely identifies a device or resource connected to the Internet. According to publically available data, IP Address-1 resolves to Silver Spring, Maryland, the same town as the Apartment.

14. Based on my review of publicly-available records of the Maryland Secretary of State, I am aware of the following:

a. YENDOUKOA LAMBONI, the defendant, is listed as SEARA's resident agent.

b. The Apartment is listed as the address of SEARA, the residence of LAMBONI, the address of the resident agent of SEARA, and the return address for the filing party who submitted the materials to the Maryland Secretary of State on SEARA's behalf.

c. According to the articles of incorporation for SEARA, the business description is: "buy and sale: fridge, stove, House Kitchen Wear, Home Tools, etc."

WHEREFORE, the deponent respectfully requests that a warrant issue for the arrest of YENDOUKOA LAMBONI, the defendant, and that he be imprisoned or bailed, as the case may be.

KRISTIN M. ALLAIN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
9th day of November, 2018

HONORABLE ROBERT W. LEHRBURGER
United States Magistrate Judge
Southern District of New York